

Thème B Le Web

Chapitre 3 À la découverte du Web

Le thème B (*Le Web*) correspond aux deux chapitres suivants :

- **Chapitre 3 : À la découverte du Web**
- Chapitre 4 : Dans la peau d'un développeur web

Le chapitre 3 est indépendant des autres chapitres.

A. Le programme

Les capacités exigibles du BO pour ce chapitre sont données ci-dessous. Les autres contenus du thème *Le Web* seront traités dans le chapitre 4.

Contenus	Capacités attendues du BO traitées dans le chapitre 3	Activités / Exercices
Repères historiques	Connaître les étapes du développement du Web.	Frise p. 54-55
Hypertexte	Maîtriser les renvois d'un texte à différents contenus.	Activité 1 p. 56 Exercice 4 p. 62
URL	Décomposer l'URL d'une page. Reconnaître les pages sécurisées.	Activité 1 p. 56 Exercices 1, 2 et 3 p. 62
Requête HTTP	Décomposer le contenu d'une requête HTTP et identifier les paramètres passés.	Activité 4 p. 59
Modèle client/serveur	Inspecter le code d'une page hébergée par un serveur et distinguer ce qui est exécuté par le client et par le serveur.	Activité 3 p. 58 Exercice 8 p. 63
Paramètres de sécurité d'un navigateur	Maîtriser les réglages les plus importants concernant la gestion des cookies, la sécurité et la confidentialité d'un navigateur. Sécuriser sa navigation en ligne et analyser les pages et les fichiers.	Activité 2 p. 57 Exercices 5, 6 et 7 p. 62-63

B. QCM diagnostic p. 54

Ces questions vont instaurer le débat, ou la discussion.

Elles sont destinées à faire une évaluation diagnostic en début de chapitre et sont disponibles sur QCMCam et aux formats PDF, PPT et ODP sur le site web : https://lienbordas.fr/740171_ch03_qcm.

1	Qu'est-ce qu'une page web ? <i>Réponses :</i> A. Un formulaire d'inscription à compléter en ligne B. Un fichier composé de textes, d'images et de liens hypertextes (bonne réponse) C. Une page de livre scannée que l'on peut lire sur le Web
2	Que signifie le cadenas qui se trouve au début de l'adresse d'un site web ? <i>Réponses :</i> A. Le site web est un site sûr. B. La connexion avec le serveur est sécurisée. (bonne réponse) C. L'accès au site est protégé par un mot de passe.
3	Parmi les 4 applications suivantes, laquelle n'est pas un navigateur web ? <i>Réponses :</i> A. Google (bonne réponse) B. Chrome C. Firefox D. Safari
4	À quoi sert un cookie HTTP, enregistré dans l'ordinateur, le smartphone, ou la tablette ? <i>Réponses :</i> A. À stocker des informations sur moi. (bonne réponse) B. À stocker des images. C. À stocker des mots de passe.
5	Amélie a choisi le mot de passe suivant pour se connecter à un réseau social : « amelie2006 ». <i>Réponses :</i> A. Ce mot de passe est sécurisé car il est difficile à trouver. B. Ce mot de passe n'est pas sécurisé car il est trop long. C. Ce mot de passe est sécurisé car il est composé de lettres et de chiffres. D. Ce mot de passe n'est pas sécurisé car il est composé d'éléments personnels. (bonne réponse)

C. Frise historique p. 55

Réponses aux questions :

1. Les liens hypertextes du Web offrent une lecture interactive et non linéaire, contrairement à celle d'un livre papier. En cliquant sur ces liens, l'utilisateur peut accéder à d'autres pages du même site web ou à d'autres sites, ainsi qu'à des contenus multimédias, selon ses envies et ses besoins. La lecture devient ainsi plus dynamique, plus riche et adaptée à chacun.

2. Les applications web ont révolutionné le commerce en ligne à partir de 2010 car elles étaient optimisées pour une utilisation sur smartphone, les rendant plus faciles d'accès. Elles offraient une navigation plus fluide et interactive, enrichie par des fonctionnalités pratiques et attractives comme l'achat en un clic, les paiements sécurisés, le suivi des commandes en temps réel et les recommandations personnalisées.

3. À partir de 2010, les développeurs du Web ont dû concevoir des applications spécifiquement pour les smartphones. La taille réduite des écrans et leur interface tactile ont introduit de nouvelles contraintes en matière de programmation. L'une des solutions les plus populaires a été le *responsive design*, qui permet à un même site de s'adapter automatiquement à la plupart des tailles d'écran (smartphone, tablette, ordinateur...) et à différents modes de navigation (écran tactile, souris...).

D. Description des activités

Activité 1 p. 56 Comment surfer sur le Web en toute sécurité ?

Capacités travaillées :

- Maîtriser les renvois d'un texte à différents contenus.
- Décomposer l'URL d'une page.
- Reconnaître les pages sécurisées.

Tout d'abord, côté vocabulaire, il convient de parler de site web (w en minuscule) et non pas de site Internet. On parle également de page web (w minuscule) et non pas de page Internet. Le Web (avec une majuscule) désigne un ensemble de pages web, reliées par des liens hypertextes.

Une page web est un fichier informatique composé de textes, d'images, de vidéos et de liens hypertextes. Grâce aux liens hypertextes, on peut naviguer de page web en page web par un simple clic de souris (sur un ordinateur) ou en tapotant avec le bout du doigt (sur un smartphone ou une tablette).

Pour naviguer sur le Web, il faut utiliser un logiciel appelé navigateur web, tel que Chrome, Edge, Safari, Firefox, Opera, etc. Les élèves confondent dans une large majorité « navigateur web » et « moteur de recherche », notamment Google (en tant que moteur de recherche) et Google Chrome. Mais le fait que l'on puisse faire une recherche sur le Web (et non pas une recherche sur Internet) en saisissant le mot recherché dans la barre d'adresse d'un navigateur est certainement à l'origine de cette confusion : la barre d'adresse sert à la fois pour faire une recherche et pour atteindre une page, si l'on connaît son adresse URL.

Le cadenas situé devant une adresse URL indique que la connexion est sécurisée. Par « sécurisée », il faut entendre que les échanges d'informations entre le client (le navigateur web) et le serveur (le serveur web distant) sont chiffrés. Néanmoins, il peut toujours s'agir d'un site pirate de *phishing*, destiné à recueillir les précieuses informations de l'utilisateur, en se faisant passer pour sa banque ou son opérateur de téléphonie mobile, par exemple. On peut donc être connecté de manière sécurisée à un site pirate. Le cadenas n'offre aucune garantie de sécurité concernant l'identité du site web consulté.

Chaque page web possède une adresse unique sur le Web, appelée URL (*Uniform Resource Locator*) qui commence par le protocole utilisé (non sécurisé « <http://> » ou sécurisé « <https://> »). Le « s » de « [https](https://) » signifie que la connexion est sécurisée, identifiée par le cadenas. HTTP est un protocole de communication établi entre le client et le serveur : c'est un ensemble de règles protocolaires.

La mention « <https://> » et « [www.](http://www) » sont parfois omis : ils sont sous-entendus. D'ailleurs, certains sites web sont accessibles sans mettre la mention « [www.](http://www) ».

Réponses aux questions :

1. Comme noms de navigateurs web, on peut citer Google Chrome, Safari, Mozilla Firefox, Opera, Microsoft Edge, Brave, Vivaldi, Tor Browser...

2. Comme noms de moteurs de recherche, on peut citer Google, le plus utilisé dans le monde, Bing de Microsoft, Yahoo!, Quant, moteur de recherche français et respectueux de la vie privée, DuckDuckGo connu pour ne pas tracer les internautes, Ecosia qui finance la plantation d'arbres...

3. a. lien 3

b. lien 4

c. lien 1

d. lien 5

e. lien 2

4. En survolant le lien Fairephone.fr avec la souris, le navigateur affiche l'URL vers laquelle pointe le lien qui est : <https://promo-fairephone.manuel-snt.fr/web/promo.html>. Le site vers lequel pointe le lien n'est pas le site officiel de la marque, donc cela ne semble pas prudent de cliquer sur ce lien.

5. Après avoir cliqué sur le lien Fairephone.fr, l'URL qui s'affiche dans la barre d'adresse du navigateur est <https://promo-fairephone.manuel-snt.fr/web/promo.html>.

6. Dans l'adresse promo-fairephone.manuel-snt.fr, le nom de domaine est manuel-snt et le sous-domaine est promo-fairephone. Le nom de domaine du site officiel est Fairephone donc l'adresse promo-fairephone.manuel-snt.fr n'est pas le site officiel de la marque. Le lien envoie sur le site du manuel SNT.

7. Comme il ne s'agit pas du site officiel de la marque, il est vivement conseillé à Fanny de ne pas y acheter son smartphone, ce site pouvant être une arnaque. Les risques possibles sont d'acheter une contrefaçon ou un produit d'occasion non signalé, ou encore un produit non garanti. Le site peut aussi avoir pour seul objectif de voler les données bancaires de Fanny (*phishing*).

8. La mention « HTTPS » est bien présente au début de l'URL, ce qui signifie que les échanges de données entre l'utilisateur et le serveur web sont sécurisés. Pourtant, le site n'est pas fiable donc le cadenas et la mention « HTTPS » ne garantissent pas la fiabilité d'un site de vente en ligne.

Activité 2 p. 57 Comment paramétrer son navigateur pour surfer en toute sécurité ?

Capacités travaillées :

- Maîtriser les réglages les plus importants concernant la gestion des cookies, la sécurité et la confidentialité d'un navigateur.
- Sécuriser sa navigation en ligne et analyser les pages et fichiers.

Lorsqu'on navigue sur le Web, les sites web nous demandent souvent lors d'une première visite l'autorisation de stocker des cookies sur notre machine. Ces cookies renferment des informations qui nous concernent. Il en existe différentes catégories : cookies de fonctionnement, cookies d'analyse, cookies liés aux réseaux sociaux, cookies de ciblage publicitaire, etc.

On peut s'opposer au stockage de ces cookies de suivi grâce au RGPD, mais certains d'entre eux sont nécessaires au bon fonctionnement du site (gestion de la session utilisateur). Il est toujours possible de consulter la nature des cookies stockés dans la mémoire du navigateur web, ou de les supprimer en accédant aux options du navigateur. Il est d'ailleurs intéressant de demander aux élèves de les supprimer manuellement. Il faut également insister sur le fait qu'un navigateur web est paramétrable selon ses choix de navigation ou le niveau de sécurité souhaité sur le Web.

Réponses aux questions :

1. Noah n'est pas obligé d'accepter les cookies de ce site : il peut tous les refuser ou n'autoriser que certains types de cookies.
2. On ferme la page web, puis on supprime les cookies du navigateur.
3. Le paramétrage des cookies est à nouveau proposé.
4. Les seuls cookies indispensables sont généralement les cookies fonctionnels.
5. Pour limiter la collecte de données de navigation par les sites web, on peut conseiller à Noah d'autoriser uniquement les cookies fonctionnels.
6. Les données qui sont enregistrées dans l'historique de navigation sont les sites web visités et les mots de passe.
7. Les paramètres du navigateur que l'on peut configurer afin de protéger notre vie privée sont :
 - la gestion des cookies ;
 - l'historique de navigation ;
 - le contrôle des accès à la localisation, à la caméra, au microphone ;
 - l'enregistrement des mots de passe ;
 - l'enregistrement des informations de formulaire ;
 - l'enregistrement des informations bancaires.
8. L'adresse IP de Noah ne change pas lorsqu'il surfe sur le Web en navigation privée.

9. Même en navigation privée, Noah laisse des traces de son passage sur le Web, par exemple chez son fournisseur d'accès à Internet qui a connaissance des sites qu'il a visités, sur les serveurs des sites web consultés qui peuvent stocker l'historique de son activité, ou bien sur le réseau interne de son lycée.

10. Pour limiter la collecte des données de navigation par les sites web, les paramètres de confidentialité et de sécurité que l'on peut activer sur son navigateur sont :

- bloquer les cookies tiers ;
- effacer automatiquement les données de navigation ;
- utiliser la navigation privée.

11. Une bonne pratique à adopter lorsqu'on surfe sur le Web depuis un appareil qui n'est pas le sien ou lorsqu'on se connecte à Internet via un réseau public est d'utiliser la navigation privée.

12. Même avec la navigation privée, il est impossible de naviguer sur le Web sans laisser de traces.

Activité 3 p. 58 Comment distinguer ce qui est exécuté par le client et le serveur ?

Capacité travaillée :

- Inspecter le code d'une page hébergée par un serveur et distinguer ce qui est exécuté par le client et par le serveur.

Cette activité porte sur une page web indiquant l'heure de Paris et l'heure de New York sur deux pendules. Après avoir affiché la page, les élèves découvrent que seule la pendule de Paris égrène les secondes : celle indiquant l'heure de New York est figée. Si on actualise la page (touche F5), l'heure de New York est alors mise à jour.

Les élèves doivent s'interroger sur la différence de programmation utilisée pour chacune des pendules. Il est important qu'ils fassent le lien entre la mise à jour de l'heure de New York et le rafraîchissement de la page web.

La pendule de Paris est codée en JavaScript, code qui est exécuté côté client, tandis que la pendule de New York est codée en PHP, code qui est exécuté côté serveur.

Réponses aux questions :

1. Lorsqu'on demande l'affichage d'une page web sur un site, le rôle de client est joué par le navigateur de l'internaute et celui de serveur par le serveur web du site.

2. a. La page indique l'heure à Paris et à New York. Mais l'heure de Paris est actualisée chaque seconde (le temps défile normalement), tandis que l'heure de New York est figée.

b. Après actualisation de la page web, l'heure de New York est mise à jour lors du chargement de la page.

3. On télécharge le fichier `pendules.php` et on l'ouvre avec un éditeur de texte.

4. a. Dans le fichier téléchargé, on remarque que la fonction `showTime()` est définie entre les balises `<script type="text/javascript">` et `</script>`, donc elle est écrite en langage JavaScript.

b. Comme cette partie du code est écrite en langage JavaScript, qui est un langage de programmation côté client, elle est exécutée côté client.

5. a. Comme la ligne `echo date("H:i:s")` se situe entre les balises `<?php` et `?>`, l'heure de New York est écrite en langage PHP.

b. Comme cette partie du code est écrite en langage PHP, qui est un langage de programmation côté serveur, elle est exécutée côté serveur.

6. Le client (le navigateur web) demande l'affichage de la page `pendules.php`. Le serveur web interprète la page web `pendules.php` et renvoie une page web décrite en HTML, en insérant l'heure de New York sous forme statique. Seul un rafraîchissement de la page permettra de mettre l'heure de New York à jour, en redemandant au serveur de renvoyer une nouvelle page web.

Activité 4 p. 59 Que contient une requête HTTP ?

Capacité travaillée :

- Décomposer le contenu d'une requête HTTP et identifier les paramètres passés.

Dans le modèle client-serveur, le client (le navigateur web) effectue une requête (une demande) au serveur (web). En réponse à cette requête, le serveur renvoie la page web demandée ou une erreur du type 404 si la page demandée n'existe pas. D'autres codes de réponse existent, les groupes de code 2xx correspondent à un succès et 3xx à une redirection.

En utilisant l'interface conçue pour cette activité, il est possible de visualiser le contenu d'une requête HTTP. Ce type de requête contient de nombreuses informations comme le navigateur utilisé, le système d'exploitation, la langue préférée de l'utilisateur ou encore l'URL de la dernière page web visitée (*Referer*). L'interface proposée affiche les informations réelles de l'élève effectuant la manipulation, afin de lui faire prendre conscience des données qu'il transmet aux serveurs.

Réponses aux questions :

1. On remplit le formulaire et on clique sur le bouton.

2. La méthode HTTP utilisée est GET.

L'URL est `https://ref.lect.manuel-snt.fr:8443/?login=Noah&password=123456`.

Les paramètres demandés sont `login = Noah` et `password=123456`.

3. La méthode HTTP utilisée est POST.

L'URL est `https://ref.lect.manuel-snt.fr:8443/`.

Les paramètres demandés sont login=Noah&password=123456.

4. Avec la méthode GET de la première requête, on voit dans l'URL le login et le mot de passe de Noah en clair, alors qu'avec la méthode POST, le login et le mot de passe de Noah sont uniquement dans le corps de la requête. Par conséquent, pour transmettre au serveur un login et un mot de passe, il est préférable d'utiliser la méthode POST.

5. La liste des données envoyées dans l'en-tête HTTP de la requête 2 est composée de toutes les lignes affichées dans l'interface de l'activité sauf la dernière. Ces données dépendent de l'internaute qui effectuent la manipulation. Voici un exemple de ce qui peut être affiché :

```
Host: ref.lect.manuel-snt.fr:8443
Connection: keep-alive
Content-Length: 26
Cache-Control: max-age=0
sec-ch-ua: "Not)A;Brand";v="8", "Chromium";v="138", "Google Chrome";v="138"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Windows"
Origin: https://www.manuel-snt.fr
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/138.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,
application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://www.manuel-snt.fr/
Accept-Encoding: gzip, deflate, br, zstd
Accept-Language: en-US,en;q=0.9,fr;q=0.8
```

6. Les données personnelles sont :

- le système d'exploitation du client ;
- le navigateur de l'internaute ;
- la langue ;
- le site d'où vient le lien donc <https://www.manuel-snt.fr/>.

7. Comme on vient de le voir dans la réponse à la question précédente, des données personnelles sont fournies au serveur auquel on se connecte en envoyant une requête HTTP.

8. Lorsque Noah surfe sur le Web, il laisse donc des traces sur les serveurs web qu'il consulte.

E. Description des exercices

Exercice 1 p. 62 Décomposition d'une URL

Capacités travaillées :

- Décomposer l'URL d'une page.
- Reconnaître les pages sécurisées.

1. a. L'URL `https://supersite.info/com` est correcte.
b. L'URL `supersite.it/com/top` est correcte.
c. L'URL `supersite-letop-org` n'est pas correcte puisqu'il manque le point séparateur entre le nom de domaine et le domaine principal.
d. L'URL `https:supersite.letop.org` n'est pas correcte puisqu'il manque « // » entre « https » et « : ».
e. L'URL `http://supersite.it/fr` est correcte.
f. L'URL `hppts://supersite.letop.org` n'est pas correcte puisque « https » est mal orthographié.
2. Pour l'URL `https://supersite.info/com` :
 - protocole de communication : https
 - nom de domaine : supersite
 - chemin d'accès : /comPour l'URL `supersite.it/com/top` :
 - nom de domaine : supersite
 - chemin d'accès : /com/topPour l'URL `http://supersite.it/fr` :
 - protocole de communication : http
 - nom de domaine : supersite
 - chemin d'accès : /fr
3. La seule URL qui pointent vers des pages sécurisées est `https://supersite.info/com` car le protocole spécifié est HTTPS.

Exercice 2 p. 62 Cybersécurité

Capacités travaillées :

- Décomposer l'URL d'une page.
- Reconnaître les pages sécurisées.

1. Avant de cliquer sur un lien contenu dans un e-mail, il est essentiel d'adopter une attitude prudente pour éviter toute tentative de *phishing*, à plus forte raison quand cet e-mail contient un message urgent incitant le destinataire à agir rapidement. La bonne attitude est de vérifier l'expéditeur de l'e-mail, de survoler le lien afin d'afficher son adresse réelle en bas à gauche du navigateur (ou dans la petite fenêtre qui s'ouvre si on utilise un logiciel de messagerie électronique) et de s'assurer qu'il renvoie bien vers le site officiel.

2. Comme Zoé n'a pas adopté l'attitude précédente, elle ne doit fournir aucune information à ce site, et surtout pas d'identifiant, de mot de passe ou de données bancaires.

3. Afin de s'assurer d'aller sur le site officiel du service de musique, Zoé doit saisir l'URL du site officiel ou la chercher dans un moteur de recherche.

Exercice 3 p. 62 Reconnaître une page sécurisée

Capacités travaillées :

- Décomposer l'URL d'une page.
- Reconnaître les pages sécurisées.

1. Pour l'URL <https://www.mabanque.fr/connexion> :

- le protocole utilisé est https
- le domaine principal est fr
- le nom de domaine est mabanque
- le nom du sous-domaine est www
- le chemin d'accès est /connexion

2. a. L'URL <https://www.mabanque.fr/> renvoie vers le même site web.

b. L'URL <https://www.ma-banque.fr/> ne renvoie pas vers le même site web car le nom de domaine de cette URL est « ma-banque » et non « mabanque ».

c. L'URL <https://compte.mabanque.fr/> renvoie vers le même site web.

d. L'URL <https://www.mabanque.com/connexion> ne renvoie pas vers le même site web car le nom de domaine principal de cette URL est « com » et non « fr ».

3. Dans cette URL, le nom de domaine est « ma-banque » et non « mabanque », donc elle renvoie vers un autre site web. Il n'est donc pas prudent de s'y connecter.

Exercice 4 p. 62 Vers quoi renvoient ces liens ?

Capacité travaillée :

- Maîtriser les renvois d'un texte à différents contenus.

a. L'URL lesupersite.it/index.html renvoie vers un fichier texte au format HTML qui n'est pas stocké dans le site web lesupersite.fr, car le domaine principal est « it » au lieu de « fr ».

b. L'URL www.lesupersite.fr/top.jpeg renvoie vers un fichier image au format JPEG qui est stocké dans le site web lesupersite.fr.

c. L'URL wwwlesupersite.fr/top.pdf renvoie vers un fichier au format PDF qui n'est pas stocké dans le site web lesupersite.fr, car le nom de domaine est « wwwlesupersite » au lieu de « lesupersite ».

d. L'URL lessupersite.fr/top/doc.html renvoie vers un fichier texte au format HTML qui n'est pas stocké dans le site web lesupersite.fr, car le nom de domaine est « lessupersite » au lieu de « lesupersite ».

e. L'URL lesupersite.fr/photo.png renvoie vers un fichier image au format PNG qui est stocké dans le site web lesupersite.fr.

Exercice 5 p. 62 Acheter un billet d'avion sur le Web

Capacité travaillée :

- Maîtriser les réglages les plus importants concernant la gestion des cookies, la sécurité et la confidentialité d'un navigateur.

Lors d'une recherche sur le Web, les sites web que nous consultons peuvent laisser des traces sur notre machine, notamment sous forme de cookies, de telle sorte que si nous y retournons ultérieurement, ces sites nous reconnaissent. Il leur est donc possible de nous proposer de la publicité ciblée ou d'augmenter le prix d'un billet d'avion. La suppression des cookies remet à zéro cette identification, si bien que le site web ne reconnaît plus le client connecté : les publicités ne sont plus ciblées et il n'est pas rare que les prix en ligne baissent.

1. Les sites web que Lucien a consultés ont très certainement stocké des cookies sur sa machine, ce qui leur permet de l'identifier lors de ses visites ultérieures. Ils peuvent donc lui proposer une publicité ciblée en relation avec ce qu'il a cherché.

2. Non, ce n'est pas le fruit du hasard. Les cookies laissés sur sa machine peuvent détecter que Lucien est intéressé par des billets d'avion. C'est pourquoi le site marchand peut être tenté d'augmenter ses tarifs pour déclencher un acte d'achat.

3. Pour résoudre son problème, Lucien pourrait supprimer tous les cookies de son ordinateur, naviguer sur le Web en ouvrant une fenêtre de navigation privée, ou encore utiliser un autre appareil pour se connecter à Internet.

Exercice 6 p. 63 Utilisez-vous des mots de passe forts sur le Web ?

Capacité travaillée :

- Maîtriser les réglages les plus importants concernant la gestion des cookies, la sécurité et la confidentialité d'un navigateur.

1. Nous avons choisi de poser cette question aux élèves afin qu'ils prennent conscience de la nécessité de sécuriser leur partage de connexion Wi-Fi.

2. Nous avons choisi de poser cette question aux élèves afin qu'ils prennent aussi conscience de la nécessité de sécuriser l'accès à leurs comptes sur les réseaux sociaux. Le risque encouru est qu'une personne malveillante puisse accéder à leurs comptes et y poster des messages ou des photos dans le but de leur nuire.

3. Avec cette question, nous espérons que les élèves se rendront compte de la nécessité d'utiliser des mots de passe différents pour chaque application.

4. Pour sécuriser son usage d'un navigateur web, il est important d'utiliser des mots de passe forts et différents pour chaque application utilisée.

Exercice 7 p. 63 Générer un mot de passe fort de façon aléatoire

Capacités travaillées :

- Boucles bornées et non bornées.
- Définitions et appels de fonctions.

1. La ligne 5 complétée est `chaine_chiffres = '0123456789'`.

2. La boucle bornée ajoute par concaténation un caractère aléatoire au hasard de la variable `chaine_chiffres` par passage dans la boucle. Comme la variable `chaine_chiffres` contient des chiffres et que la boucle s'exécute trois fois, ces deux lignes ajoutent trois chiffres aléatoires à la chaîne de caractères vide `mot`. À la fin de l'exécution de ces deux lignes, la variable `mot` contient trois chiffres aléatoires.

3. La ligne 12 ajoutée avant l'instruction `return mot` est :

```
mot = mot + choice(chaine_minuscules)
```

4. On vérifie que la fonction `mot_de_passe_fort()` a bien le comportement attendu.

5. Pour ajouter au mot de passe trois lettres majuscules, il faut ajouter cette ligne 13 avant l'instruction `return mot` : `mot = mot + choice(chaine_majuscules)`

Pour ajouter au mot de passe trois caractères spéciaux, il faut ajouter cette ligne 14 avant l'instruction `return mot` : `mot = mot + choice(chaine_speciaux)`.

La correction dans l'éditeur WebPython est disponible à cette adresse :

https://lienbordas.fr/740171_webpython13_XKT.

Exercice 8 p. 63 Minage de Bitcoin à votre insu

Capacité travaillée :

- Inspecter le code d'une page hébergée par un serveur et distinguer ce qui est exécuté par le client et par le serveur.

1. Le minage de Bitcoin consiste à valider les transactions effectuées et à les regrouper dans des blocs. Cette opération requiert une grande puissance de calcul car elle doit résoudre des problèmes mathématiques très complexes, ce qui consomme beaucoup d'électricité et peut nécessiter du matériel informatique spécialisé. Le premier internaute qui trouve la solution ajoute un bloc à la blockchain et reçoit une récompense en bitcoins.

2. Le script JavaScript est exécuté par le client.

3. Si un pirate parvient à miner du Bitcoin sur un autre ordinateur que le sien, il n'a pas besoin d'acheter de matériel ni de payer la consommation d'électricité. En outre, s'il arrive à trouver la solution et ajoute un bloc à la blockchain, il est récompensé sans avoir dépensé d'argent.

Exercice 9 p. 63 Écologie

Capacité transversale travaillée :

- Faire un usage responsable et critique des sciences et technologies numériques.

1. Laisser un ordinateur allumé en permanence nécessite de l'électricité. Chez un hébergeur, un serveur est aussi allumé en continu mais il héberge également d'autres sites web. La solution de louer un hébergement chez un hébergeur Internet est donc plus écologique.

2. Il est préférable de choisir un hébergeur proche des utilisateurs du site web afin de minimiser la distance des échanges entre les utilisateurs et le serveur.

3. Si Louka réduit la taille des images et des vidéos, le volume de données échangées entre le serveur et les utilisateurs sera moins important, ce qui réduira son impact environnemental.

F. Bilan du chapitre p. 64

Question	Réponse
1	c. Le nom de domaine.
2	c. Accéder à une sous-section spécifique d'un site web.
3	b. Un sous-domaine du site web.
4	a. http://www.sitetop.com/chemin
5	c. HTTPS est sécurisé, HTTP ne l'est pas.
6	b. L'orthographe du nom de domaine.
7	a. Le chiffrement des données échangées.
8	a. Un élément cliquable qui permet de naviguer vers une autre ressource.
9	c. Le navigateur affiche l'URL du lien.
10	b. Pour vérifier qu'il ne mène pas à un site frauduleux.
11	a. L'accès à la localisation et à la caméra.
12	b. Les cookies fonctionnels.
13	c. Empêcher la conservation de l'historique de navigation.
14	b. Utiliser la navigation privée.
15	b. Afficher des pages web.

Des QCM d'auto-évaluation sont disponibles pour un travail en autonomie de l'élève à l'adresse : https://lienbordas.fr/740171_ch03_bilan.